



HOUSE COMMITTEE *on* APPROPRIATIONS  
RANKING MEMBER ROSA DeLAURO

## **Strengthening Cybersecurity**

### ***Cybersecurity Provisions in the Fiscal Year 2023 Consolidated Appropriations Act***

Democrats in Congress have been fighting to secure transformative federal investments to help fight inflation, lower the cost of living, support working families, create American jobs, and combat climate change.

In December 2022, Democrats in Congress secured transformative investments in the 2023 federal funding bill that help the middle class, working families, small businesses, and the vulnerable who work hard. Instead of catering to the biggest corporations and billionaires, we are tackling some of our nation's biggest challenges including protecting Americans with historic investments in cyber security.

Overall, the 2023 funding bill provides more than \$16.5 billion to bolster cybersecurity efforts. Below you will find a summary of all the cybersecurity, cyberspace operations, and cyber research and development provisions included in the fiscal year 2023 Consolidated Appropriations Act.

#### **Defense**

The fiscal year 2023 spending bill includes:

- \$11.2 billion for cybersecurity, cyberspace operations, and cyber research and development activities, including:
  - \$6.6 billion for network modernization, encryption solutions, infrastructure defense, Zero Trust architecture, and other increased and improved network protections.
  - \$4.2 billion for cyberspace operations that include cyber collection, cyber effects operations, the resiliency of key systems, and support for the Cyber Mission Force teams.
  - \$400 million for research in key cyber-related areas including network resilience.

#### **Homeland Security**

The bill includes increased investments in cybersecurity, including:

- \$1.76 billion for the Cybersecurity and Infrastructure Security Agency, including:
  - \$1.3 billion for cybersecurity operations.
  - \$454.1 million for the acquisition of cybersecurity technologies.
- \$102.7 million for department-wide cybersecurity enhancements.

- \$3 million for the Cybersecurity and Diversity Fellowship program.
- \$4 million for the Transportation Security Administration for pipeline cybersecurity.

## **Commerce, Justice, Science, and Related Agencies**

The fiscal year 2023 bill provides significant resources to help ensure the security of information technology systems, take action to prevent and respond to cyber intrusions and attacks, and pursue criminals and national security threats that threaten the safety, economic well-being and security of Americans.

### Department of Commerce (DOC)

The fiscal year 2023 bill includes \$127.5 million for DOC cybersecurity investments and programs, an increase of \$42.5 million above fiscal year 2022, as follows:

- \$92.5 million for the National Institute of Standards and Technology (NIST) to support and strengthen Federal and private cybersecurity efforts, an increase of \$7.5 million above fiscal year 2022; and
- \$35 million for the Department's Nonrecurring Expenses Fund to support cybersecurity risk mitigation efforts at the Department.

### Department of Justice (DOJ)

The fiscal year 2023 bill includes \$174.2 million for DOJ cybersecurity investments and programs, an increase of \$109.4 million above fiscal year 2022, as follows:

- \$138 million for DOJ-wide systems security, an increase of \$100 million above fiscal year 2022.
- \$16.2 million for the National Security Division to pursue cyber intrusions and other security threats.
- \$13 million for the Office of Justice Programs for Economic, High-tech, White Collar and Cybercrime Prevention grants.
- \$7 million for the Office of Justice Programs for a cybercrime enforcement grant program, and for a National Resource Center on Cybercrimes Against Individuals to provide resource information, training, and technical assistance to improve the capacity of individuals, organizations, governmental entities, and communities to prevent, enforce, and prosecute cybercrimes against individuals.

### National Science Foundation

- \$69 million for the National Science Foundation's CyberCorps Scholarships for Service program, an increase of \$6 million above fiscal year 2022, to help recruit and train the next generation of U.S. cybersecurity professionals.

## **Financial Services and General Government**

The bill provides:

- \$100 million for the Department of the Treasury Cybersecurity Enhancement Account to protect the Department's critical IT infrastructure from cyberattacks.
- \$75 million for Election Security Grants to support State efforts to improve the security and integrity of elections for Federal office, including cybersecurity.
- \$278 million for the Internal Revenue Service to protect taxpayers' personnel identification and tax data as well as secure and modernize IRS systems and networks to prevent cyberattacks.
- \$114 million for the Judiciary to better secure sensitive case data for the lower courts and the Supreme Court from cyberattacks.
- \$19 million for the Office of Personnel Management to enhance cyber security protection by increasing their Zero Trust framework and modernizing IT systems to better protect sensitive federal annuitant and prospective employee data from cyber thieves.
- \$22 million for the Office of the National Cyber Director to continue to stand up the new Office of the National Cyber Director to help coordinate Federal cybersecurity policy and strategy.

## **State and Foreign Operations**

This bill includes:

- \$389 million for the State Department Capital Investment Fund and \$259 million for the USAID Capital Investment Fund to support enterprise-level investments in information technology (IT) modernization and essential IT services and to address cybersecurity vulnerabilities at the Department of State and USAID.
- \$30 million to protect independent media and activists overseas, including online security.
- \$90.5 million, a \$13 million increase above fiscal year 2022, to promote global internet freedom. This funding includes \$40 million, a \$13 million increase above fiscal year 2022, for the Open Technology Fund which supports technologies to protect journalists, civil society, and audiences from surveillance, censorship, and digital attacks from repressive actors and governments.

## **Energy & Water Development**

This bill includes:

### U.S. Army Corps of Engineers

- \$4 million for Cybersecurity in the Operation and Maintenance account, to provide services related to agency-wide cybersecurity work in support of the Civil Works mission.

### Department of Energy

- \$200 million for the Office of Cybersecurity, Energy Security, and Emergency Response, an increase of \$14 million above fiscal year 2022.
- \$446 million for the National Nuclear Security Administration's Office of Information Technology and Cyber Security, an increase of \$39 million above fiscal year 2022.

## **Transportation-Housing & Urban Development**

The fiscal year 2023 bill:

### Department of Transportation (DOT)

- Provides \$48.1 million, \$8.7 million above fiscal year 2022, for DOT's Cyber Security Initiatives to support enhancements and improvements to the security of the network and reduce the risk of security breaches.
- Includes \$25 million, equal to the budget request, for FAA's Operations account for 26 new positions, and \$4.8 million for FAA's Research, Engineering, and Development account, to protect against threats to national airspace operations.
- Directs DOT to consider projects that include testing the cybersecurity of global navigation satellite systems as part of its autonomous vehicles research plan to improve vehicle and road safety.
- Provides \$63 million for the Federal Motor Carrier Safety Administration's information technology modernization, including to mitigate cybersecurity threats of its own systems and to support its share of DOT investments in cybersecurity.
- Supports the use of fiscal year 2023 funding to help facilitate the execution of Amtrak's existing active cyber defense strategy, including the use of cyber deception capabilities, which is consistent with NIST cybersecurity guidelines and research and development with Federally funded research and development centers.
- Directs the Washington Metropolitan Area Transit Authority to comply with cybersecurity best practices and expand its cybersecurity plan analysis.
- Invests \$3 million through the Highway Trust Fund to address transit cybersecurity, including identifying vulnerabilities, threats, and risks and assessing and developing solutions that transit agencies can implement.
- To enhance pipeline safety, the Pipeline and Hazardous Materials Safety Administration (PHMSA) is provided \$8 million for training, information-sharing, and community assistance services. This includes Security and Cyber Training for Federal and state pipeline inspectors and investigators to improve their understanding of cyber hygiene and proper security and cyber protocols to help prevent cyber incidents such as the 2021 Colonial Pipeline attack.
- Provides \$4.9 million to PHMSA for information technology investments, including improved cybersecurity in all of the agency's mission systems.

- Requires the DOT Secretary to work with the Secretary of Homeland Security to ensure best practices for Industrial Control Systems Procurement are up-to-date and that systems procured with funds provided to DOT by this bill are purchased using such practices.

#### Department of Housing and Urban Development (HUD)

- Provides \$374.7 million, \$51.6 million above fiscal year 2022, for HUD's Information Technology Fund to support all IT systems and applications, including cybersecurity.

#### **Military Construction & Veterans Affairs**

The fiscal year 2023 bill provides \$400 million to support enterprise-wide cybersecurity efforts at the Department of Veterans Affairs (VA). These funds will support ongoing efforts to monitor, detect, and mitigate risks and threats to VA's network and infrastructure as well as secure access to protected data. These funds will allow VA to invest in new, proven technologies to adapt to the evolving cybersecurity threat landscape.

#### **Labor-HHS-Education**

The fiscal year 2023 funding bill includes \$100 million, an increase of \$29 million over fiscal year 2022 levels, for the Department of Health and Human Services to enable better prevention, detection, assessment, and remediation of cybersecurity threats.

#### **Agriculture-Rural Development- FDA**

The 2023 bill invests:

- No less than \$77.4 million for departmental cyber security activities.
- An increase of \$5 million to build a permanent medical device cybersecurity program at the FDA.